

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 10307776 A

(43) Date of publication of application: 17.11.98

(51) Int. Cl.

G06F 13/00

G06F 9/06

(21) Application number: 09115634

(71) Applicant: NEC NIIGATA LTD

(22) Date of filing: 06.05.97

(72) Inventor: YOKOYAMA MASATOSHI

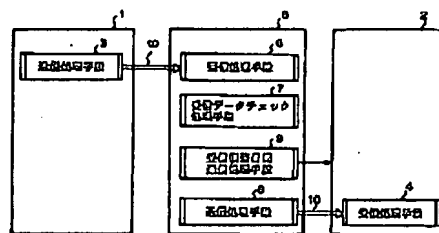
(54) COMPUTER VIRUS RECEPTION MONITOR
DEVICE AND ITS SYSTEM

COPYRIGHT: (C)1998,JPO

(57) Abstract:

PROBLEM TO BE SOLVED: To automatically prevent a reception-side device from being infected with a computer virus through data communication between computers by making a computer virus check on communication data and informing the reception-side device that a computer virus has been detected in such a case.

SOLUTION: When a transmission-side device 1 sends communication data 10 to the reception-side device 2, the computer virus reception monitor device 5 receives it through a receiving process means 6 before the reception-side device 2 receives the communication data 10. The communication data 10 taken in by the computer virus reception monitor device 5 are checked by a receive data check process means 7 as to a computer virus. If the communication data 10 are infected with a computer virus and illegal, a receive data check process means 7 discards the communication data 10 and informs the reception-side device 2 that the infected illegal data has been sent.



(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 10307776 A

(43) Date of publication of application: 17.11.98

(51) Int. Cl.

G06F 13/00

G06F 9/06

(21) Application number: 09115634

(71) Applicant: NEC NIIGATA LTD

(22) Date of filing: 06.05.97

(72) Inventor: YOKOYAMA MASATOSHI

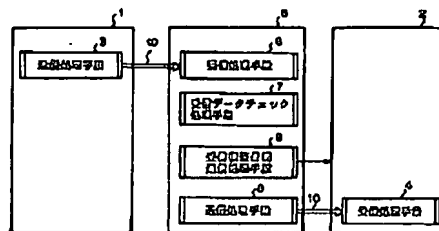
(54) COMPUTER VIRUS RECEPTION MONITOR
DEVICE AND ITS SYSTEM

COPYRIGHT: (C)1998,JPO

(57) Abstract:

PROBLEM TO BE SOLVED: To automatically prevent a reception-side device from being infected with a computer virus through data communication between computers by making a computer virus check on communication data and informing the reception-side device that a computer virus has been detected in such a case.

SOLUTION: When a transmission-side device 1 sends communication data 10 to the reception-side device 2, the computer virus reception monitor device 5 receives it through a receiving process means 6 before the reception-side device 2 receives the communication data 10. The communication data 10 taken in by the computer virus reception monitor device 5 are checked by a receive data check process means 7 as to a computer virus. If the communication data 10 are infected with a computer virus and illegal, a receive data check process means 7 discards the communication data 10 and informs the reception-side device 2 that the infected illegal data has been sent.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-307776

(43) 公開日 平成10年(1998)11月17日

(51) IntCl.⁹

G 0 6 F 13/00
9/06

識別記号

3 5 1
5 5 0

F I

G 0 6 F 13/00
9/06

3 5 1 Z
5 5 0 Z

審査請求 有 請求項の数 4 O L (全 5 頁)

(21) 出願番号 特願平9-115634

(22) 出願日 平成9年(1997)5月6日

(71) 出願人 000190541

新潟日本電気株式会社

新潟県柏崎市大字安田7546番地

(72) 発明者 横山 正敏

新潟県柏崎市大字安田7546番地 新潟日本
電気株式会社内

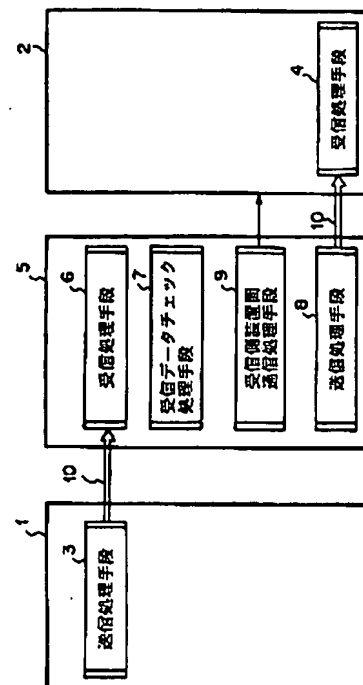
(74) 代理人 弁理士 山下 穠平

(54) 【発明の名称】 コンピュータウイルス受信監視装置及びそのシステム

(57) 【要約】

【課題】 コンピュータ回線網に接続されている受信側装置がコンピュータウイルスに感染した通信データを受信しないようにして、受信側装置のコンピュータウイルスによる感染を未然に防ぐ。

【解決手段】 コンピュータ回線網からデータを受信する受信処理手段と、前記受信処理手段により受信した受信データがコンピュータウイルスに感染しているかどうかを診断する受信データ処理手段と、前記受信データが前記コンピュータウイルスに感染している場合に、これを示す感染信号を受信側装置に知らせる受信側装置間通信処理手段と、前記受信データが前記コンピュータウイルスに感染していない場合に、前記受信データを前記受信側装置に送信する送信処理手段とを備えるコンピュータウイルス受信監視装置をコンピュータ回線網と受信側装置との間に介在させる。



【特許請求の範囲】

【請求項1】 コンピュータ回線網と前記コンピュータ回線網を通して送られてくる送信側装置からのデータを受信する受信側装置との間にあり、前記コンピュータ回線網から前記データを受信する受信処理手段と、前記受信処理手段により受信した受信データがコンピュータウイルスに感染しているかどうかを診断する受信データ処理手段と、

前記受信データが前記コンピュータウイルスに感染している場合に、これを示す感染信号を前記受信側装置に知らせる受信側装置間通信処理手段と、

前記受信データが前記コンピュータウイルスに感染していない場合に、前記受信データを前記受信側装置に送信する送信処理手段とを備えることを特徴とするコンピュータウイルス受信監視装置。

【請求項2】 前記受信データを一時記憶する作業用記憶部と、

前記コンピュータウイルスのパターンを記憶する不正データパターン記憶部と、

制御処理装置とを備え、

前記診断は、前記作業用記憶部に一時記憶されている前記受信データと前記不正データパターン記憶部に記憶されている前記コンピュータウイルスの前記パターンとを前記制御処理装置において比較することによりおこなうことを特徴とする請求項1に記載のコンピュータウイルス受信監視装置。

【請求項3】 請求項1又は2に記載のコンピュータウイルス受信監視装置より前記感染信号を受信したときには受信データを受信しないことを特徴とする受信側装置。

【請求項4】 請求項1又は2に記載のコンピュータウイルス受信監視装置及び請求項3に記載の受信側装置より構成されることを特徴とするコンピュータウイルス受信監視システム。

【発明の詳細な説明】

【0001】

【発明が属する技術分野】 本発明は、コンピュータネットワークにおける送信側装置と受信側装置との間のデータ通信を制御する通信制御装置、及びそれを含むシステムに関するものであり、特に、コンピュータウイルス受信監視装置、及びそれを含むシステムに関するものである。

【0002】

【従来の技術】 図4は特開平6-311144号公報に掲載の従来の通信制御方法を用いた処理システムの構成を示すブロック図である。図4において、401は例えばコンピュータなどの送信側装置、402は例えばコンピュータなどの受信側装置、403は送信側装置401内の送信処理を行う送信処理手段、404は受信処理装置402内の受信処理を行う受信処理手段、405は送

信処理手段403から受信処理手段404へ送信される固定長通信データ、406、407はチェック用パリティ、409は受信データチェック処理手段、410は通信初期化処理手段である。

【0003】 次に動作について説明する。固定長通信データ405にエラーチェック用パリティ406、407を設ける。送信処理手段403からの固定長通信データ405は、受信処理手段404で受信され、受信データエラーチェック処理手段409でそのデータ405のチェック用パリティ406、407をチェックすることにより正しいか否かが判定される。その固定長通信データ405が不正であった場合、通信関係の処理系は通信初期化処理手段410で初期化され、これにより通信が復旧される。

【0004】

【発明が解決しようとする課題】 従来の通信制御方法は、受信側装置402が固定長通信データの欠除を検出することにより、送信側装置401に通信データの再送を要求する、或いは、受信側装置402の再初期化を行うことにより通信データの正常性を保証するものであり、通信データが送信側装置401や受信側装置402にとって本当に無害なものかどうかをこの通信制御方法によってチェックすることができず、コンピュータウイルスに感染された通信データを受信側装置402が取り込んでしまう可能性がある。また、受信側装置402が受信したデータがコンピュータウイルスに感染しているかどうかを確認する為には、受信データに含まれるデータやプログラムを使用したり実行したりする前に、それらをコンピュータウイルスチェックプログラムによって調べなければならない。

【0005】 【発明の目的】 この発明は上記のような問題を解決するためになされたものであり、通信データが受信側装置で受信される前に、通信データに対してコンピュータウイルスチェックをかけて、コンピュータウイルスが検出された場合に、受信側装置にコンピュータウイルスが検出されたことを通知することにより、コンピュータ間のデータ通信による受信側装置のコンピュータウイルス感染を自動的に防止することができるコンピュータウイルス受信監視装置、及びそれを含むシステムを提供することを目的とする。

【0006】

【課題を解決するための手段】 本発明によるコンピュータウイルス受信監視装置は、コンピュータ回線網と前記コンピュータ回線網を通して送られてくる送信側装置からのデータを受信する受信側装置との間にあり、前記コンピュータ回線網から前記データを受信する受信処理手段と、前記受信処理手段により受信した受信データがコンピュータウイルスに感染しているかどうかを診断する受信データ処理手段と、前記受信データが前記コンピュータウイルスに感染している場合に、これを示す感染信

号を前記受信側装置に知らせる受信側装置間通信処理手段と、前記受信データが前記コンピュータウイルスに感染していない場合に、前記受信データを前記受信側装置に送信する送信処理手段とを備えることを特徴とする。

【0007】また、本発明によるコンピュータウイルス受信監視装置は、前記受信データを一時記憶する作業用記憶部と、前記コンピュータウイルスのパターンを記憶する不正データパターン記憶部と、制御処理装置とを備え、前記診断は、前記作業用記憶部に一時記憶されている前記受信データと前記不正データパターン記憶部に記憶されている前記コンピュータウイルスの前記パターンとを前記制御処理装置において比較することによりおこなうことを特徴とする。

【0008】更に、本発明による受信側装置は、上記コンピュータウイルス受信監視装置より前記感染信号を受信したときには受信データを受信しないことを特徴とする。

【0009】更に、本発明によるコンピュータウイルス受信監視システムは、上記コンピュータウイルス受信監視装置及び上記受信側装置より構成されることを特徴とする。

【0010】〔作用〕受信側装置が通信データを受信する前にコンピュータウイルス受信監視装置が自動的にコンピュータウイルスチェックを行う。このため、受信側装置は受信データにコンピュータウイルスチェックをかけることなく、受信した直後に受信データに含まれるデータやプログラムを使用できる。また、コンピュータウイルスに感染した通信データは受信側装置に到達する前に破棄されるので、受信側装置はコンピュータウイルスに感染されない。さらに、コンピュータウイルスに感染した通信データがチェック機能により検出され破棄されても、受信データがコンピュータウイルスに感染しているためにデータ破棄したことを受信側装置に通知するので、通信エラーとの区別が容易である。

【0011】

【発明の実施の形態】次に、本発明の実施の形態について図面を参照して詳細に説明する。本発明の最良の実施の形態は図1を参照すると以下ようになる。コンピュータウイルス受信監視装置5は、送信側装置1と受信側装置2との間にある。コンピュータウイルス受信監視装置5は送信側装置1からの通信データ10を受信する受信側装置2との間にある。コンピュータウイルス受信監視装置5は送信側装置1からの通信データ10を受信する受信処理手段6をもつ。また、通信データ10のコンピュータウイルス感染をチェックする受信データチェック処理手段7をもつ。送信処理手段8は受信側装置2に通信データ10を送信するためのものである。受信側装置間通信処理手段9は、受信した通信データ10がコンピュータウイルスに感染していることがコンピュータウイルスチェックにより判明した場合に、受信側装置2にコンピュータウイルスに感染している通信データの受信があったこと

を通知する為のものである。

【0012】次に図1のブロック図および図2の動作フローチャートを参照してこの実施形態の動作について説明する。送信側装置1が受信側装置2に向けて、通信データ10を送信すると、受信側装置2が通信データ10を受信する前に、受信処理手段6によりコンピュータウイルス受信監視装置5がこれを受信する（ステップS1）。コンピュータウイルス受信監視装置5に取り込まれた通信データ10は、受信データチェック処理手段7によりコンピュータウイルスチェックされる（ステップS2）。チェックの結果、通信データ10にコンピュータウイルスの感染が認められなかった場合、コンピュータウイルス受信監視装置5は送信処理手段8により通信データ10を受信処理手段4を備える受信側装置2へ送る（ステップS3）。これにより受信側装置2は通信データ10をコンピュータウイルスに感染していない通常のデータとして受信する。受信データ10がコンピュータウイルスに感染している心配がないので、ウイルスチェックをしないでデータにアクセスできる。通信データ10がコンピュータウイルスに感染していて不正であった場合、コンピュータウイルス受信監視装置5は受信データチェック処理手段7により通信データ10を破棄し（ステップS4）、受信側装置間通信手段9により受信側装置2にコンピュータウイルスに汚染されている不正データが送信されてきたことを通知する（ステップS5）。通信データ10がコンピュータウイルスに汚染されている不正データであった場合は、コンピュータウイルス受信監視装置5より受信側装置2に対して受信側装置間通信処理手段9による通知があるので、単純な通信エラーとの区別は容易である。受信側装置2は、この通知があったときには通信データを受信しない。

【0013】なお、本実施形態においては、送信側装置1と受信側装置2とをそれぞれ送信専用或いは受信専用として説明したが、送信側装置1と受信側装置2との両方の機能を持つ送受信装置が一般的な形態の装置である。

【0014】また、本実施形態の受信装置は、パソコン通信などのサーバに使用することもできる。

【0015】

【実施例】次に、本発明の実施例について図面を参照して詳細に説明する。

【0016】図3はコンピュータウイルス受信監視装置5及びその周辺の一実施例を示すブロック図である。コンピュータ回線網301を通して、図1の送信側装置1から受信側装置2にデータが送信される。制御処理装置305は図1における受信処理手段6、受信データチェック処理手段7、送信処理手段8、および受信側装置間通信手段9を制御する為のものでMPU等により構成されている。制御命令記憶部303は制御処理装置305の制御命令を記憶する為のもので、コンピュータウイルス

スの影響を排除する為にROM (Read Only Memory) により構成されている。作業用記憶部304はコンピュータ回線網301より受信した通信データ10の一時的に記憶する為に使用する為のものでRAM (Random Access Memory) により構成されている。不正データパターン記憶部302は既知のコンピュータウイルスのデータパターンを記憶しておく部分でデータパターンの追加を考慮して、PROM (Programmable Read Only Memory) により構成されている。不正データパターン記憶部302は図1の受信データチェック処理手段7として使用される。また、作業用記憶部304は図1の受信処理手段6、送信処理手段8、受信側装置間通信手段9を使用する際にも利用する。

【0017】次に図3のブロック図および図2の動作フローチャートを参照して本実施例の動作について説明する。送信側装置1がコンピュータ回線網301を通して受信側装置2に向けて、通信データ10を送信すると、受信側装置2が通信データ10を受信する前に制御命令記憶部303に記憶されているデータ受信を行う命令を制御処理装置305が実行する。その実行の度にコンピュータウイルス受信監視装置5は通信データ10を作業用記憶部304に記憶する(ステップS1)。制御処理装置305が制御命令記憶部303に記憶されている命令により不正データパターン記憶部302の不正データパターンと作業用記憶部304に記憶された通信データ10を比較する(ステップS2)。比較の結果、不正データパターンと共通のデータパターンが通信データ10に認められない場合には、コンピュータウイルスの感染はないものとして、制御処理装置305は制御命令記憶部303に記憶されている受信側装置2への通信データ10の受け渡し命令を実行し、通信データ10を送信する(ステップS3)。不正データパターンと共通のデータパターンが通信データ10が認められた場合には、通信データ10がコンピュータウイルスに感染しているとして通信データ10を破棄し(ステップS4)、制御処理装置305は制御命令記憶部303に記憶されている本体システム2への通知命令を実行し、受信側装置2に不正データが送信されてきたことを通知する(ステップS5)。

【0018】

【発明の効果】以上説明したように本発明によれば、送信側装置から受信側装置に通信データが送信された場

合、受信側装置に通信データが届く前にコンピュータウイルス受信監視装置がそのデータを受信し、コンピュータウイルスチェックを行い、コンピュータウイルスに感染されていない通信データのみを受信側装置に送信する為、受信側装置のデータ通信によるコンピュータウイルス感染を未然に防げる。また、コンピュータウイルスチェックをデータ受信時に自動的に行っていることで受信側装置がデータ受信後に改めてチェックする必要がなくなる。

【図面の簡単な説明】

【図1】本発明によるコンピュータウイルス受信監視装置、及びそれを含むデータ送受信システムの構成を示す第1のブロック図である。

【図2】本発明によるコンピュータウイルス受信監視装置の制御処理を示すフローチャートである。

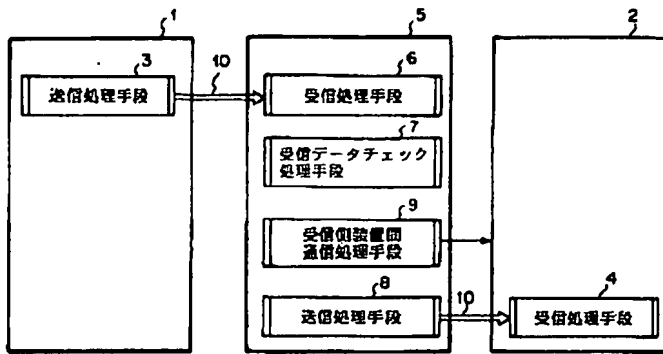
【図3】本発明によるコンピュータウイルス受信監視装置、及びそれを含むデータ送受信システムの構成を示す第2のブロック図である。

【図4】従来の通信制御方法を用いたデータ送受信システムの構成を示すブロック図である。

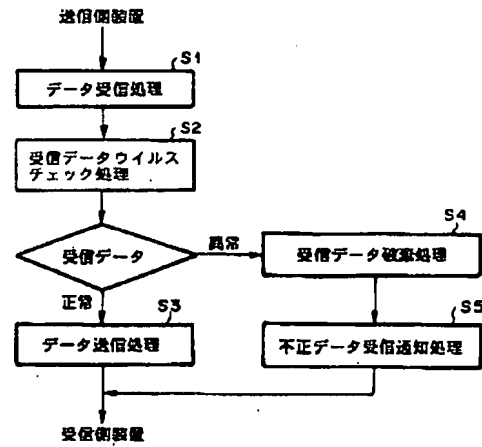
【符号の説明】

- 1 送信側装置
- 2 受信側装置
- 3 送信処理手段
- 4 受信処理手段
- 5 コンピュータウイルス受信監視装置
- 6 受信処理手段
- 7 受信データチェック処理手段
- 8 送信処理手段
- 9 受信側装置間通信処理手段
- 10 通信データ
- 301 コンピュータ回線網
- 302 不正データパターン記憶部
- 303 制御命令記憶部
- 304 作業用記憶部
- 305 制御処理装置
- S1 データ受信処理
- S2 受信データチェック処理
- S3 データ送信処理
- S4 受信データ破棄処理
- S5 不正データ受信通知処理

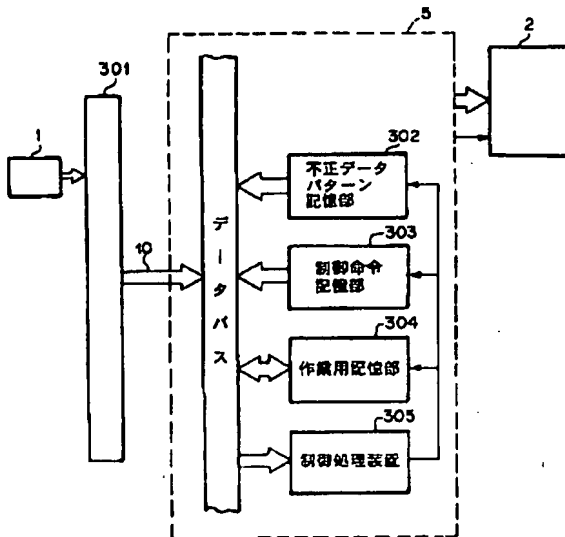
【図1】



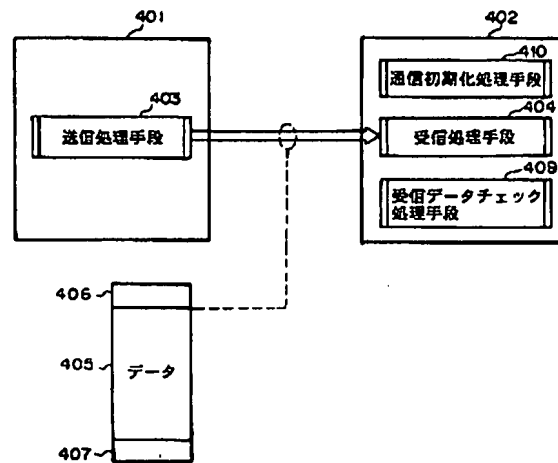
【図2】



【図3】



【図4】



10-307776

[0011]

[Embodiments] Next, an embodiment of the present invention will be described with reference to the drawings. The most preferable embodiment of the present invention will be described with reference to Fig. 1. Namely, a computer virus reception monitoring device 5 is interposed between a transmitting-side device 1 and a receiving-side device 2 that receives communication data 10 from the transmitting-side device 1. The computer virus reception monitoring device 5 includes a receiving means 6 that receives the communication data 10 sent from the transmitting-side device 1. Moreover, the computer virus reception monitoring device 5 includes a received data checking means 7 that checks if the communication data 10 is infected with a computer virus. The transmitting means 8 transmits the communication data 10 to the receiving-side device 2. If the computer virus check reveals that the received communication data 10 has been infected with a computer virus, a communicating-with-receiving-side device means 9 notifies the receiving-side device 2 that communication data infected with a computer virus has been received.

[0012] Next, the actions to be performed according to the present embodiment will be described with reference to the block diagram of Fig. 1 and the flowchart of Fig. 2. When the transmitting-side device 1 transmits communication data 10 to the receiving-side device 2, and before the receiving-side device 2 receives the communication data 10, the receiving means 6 included in the computer virus reception monitoring device 5 receives the communication data 10 (step S1). The received data checking means 7 checks if the communication data 10 fetched into the computer virus reception monitoring device 5 is infected with a computer virus (step S2). If the result of the check demonstrates that infection of the communication data 10 with a computer virus is not recognized, the transmitting means 8 included in the computer virus reception monitoring device 5 transmits

the communication data 10 to the receiving-side device 2 that includes the receiving means 4 (step S3). Consequently, the receiving-side device 2 receives the communication data 10 as normal data uninfected with a computer virus. As the receiving-side device 2 need not care about whether the received data 10 is infected with a computer virus, the receiving-side device 2 can access the data without performing a virus check. If the communication data 10 is infected with a computer virus and is regarded as illegal data, the received data checking means included in the computer virus reception monitoring device 5 discards the communication data 10 (step S4). The communicating-with-receiving-side device means 9 notifies the receiving-side device 2 that illegal data contaminated with a computer virus has arrived (step S5). If the communication data 10 is illegal data contaminated with a computer virus, the communicating-with-receiving-side device means 9 included in the computer virus reception monitoring device 5 notifies the receiving-side device of the fact. A simple communication error can therefore be readily discriminated. When the receiving-side device 2 receives the notification, the receiving-side device 2 receives no communication data.

[0013] According to the present embodiment, the transmitting-side device 1 and receiving-side device 2 are dedicated to transmission or reception. Transmitter-receivers having the capabilities of both the transmitting-side device 1 and receiving-side device 2 are generally adopted as the devices.

[0014] Moreover, the receiving-side device employed in the present embodiment may be adopted as a server on a network on which personal computers communicate with one another.

[0015]

[Examples] Next, an example of the present invention will be described with reference to the drawings.

[0016] Fig. 3 is a block diagram showing an example of the computer virus reception monitoring device 5 and its peripherals. The transmitting-side device 1 shown in Fig. 1

transmits data to the receiving-side device 2 shown therein over a computer network 301. A control unit 305 is formed with an MPU or the like in order to control each of the receiving means 6, received data checking means 7, transmitting means 8, and communicating-with-receiving-side device means 9. A control instruction sent from the control unit 305 is stored in a control instruction memory 303. The control instruction memory 303 is formed with a read-only memory (ROM) in an effort to remove the adverse effect of a computer virus. A working memory 304 is used to temporarily store communication data 10 received from the computer network 301, and formed with a random access memory (RAM). Data patterns of known computer viruses are stored in an illegal data pattern memory 302 that is formed with a programmable read-only memory (PROM) in consideration of the possibility that other data pattern may be added. The illegal data pattern memory 302 is used as the received data checking means 7 shown in Fig. 1. Moreover, the working memory 304 is utilized at the time of using the receiving means 6, transmitting means 8, and communicating-with-receiving-side device means 9.

[0017] Next, actions to be performed in the present example will be described with reference to the block diagram of Fig. 3 and the flowchart of Fig. 2. The transmitting-side device 1 transmits communication data 10 to the receiving-side device 2 over the computer network 301. Before the receiving-side device 2 receives the communication data 10, the control unit 305 executes a data reception instruction that is stored in the control instruction memory 303. Every time the instruction is executed, the computer virus reception monitoring device 5 stores the communication data 10 in the working memory 304 (step S1). In response to a instruction stored in the control instruction memory 303, the control unit 305 compares the communication data 10 stored in the working memory 304 with the illegal data patterns stored in the illegal data pattern memory 303 (step S2). If the result of the comparison demonstrates that no data pattern

identical to any of the illegal data patterns is detected in the communication data 10, the control unit 305 judges that the communication data 10 is not infected with a computer virus. The control unit 305 then executes an instruction that the communication data 10 should be handed to the receiving-side device 2 which is stored in the control instruction memory 303, and transmits the communication data 10 accordingly (step S3). If a data pattern identical to any of the illegal data patterns is detected in the communication data 10, it is judged that the communication data 10 has been infected with a computer virus. The communication data 10 is therefore discarded (step S4). The control unit 305 executes an instruction that the main system 2 should be notified which is stored in the control instruction memory 303. The control unit notifies the receiving-side device 2 that illegal data has arrived (step S5).

[0018]

[Advantages] As described above, according to the present invention, when communication data is transmitted from a transmitting-side device to a receiving-side device, before the communication data reaches the receiving-side device, a computer virus reception monitoring device receives the data and checks the data for a computer virus. Only communication data uninfected with a computer virus is transmitted to the receiving-side device. Consequently, the receiving-side device can be prevented from being infected with a computer virus through data communication. Moreover, as the computer virus check is automatically performed at the time of data reception, the receiving-side device need not check for a computer virus after receiving the data.